Quagmire ciphers and group theory:
What is a Porta cipher?

Thomas Kaeding
xnrqvat@oynpxfjna.qhpxqaf.bet (ROT13'ed to combat spam)
December, 2022

Abstract: It is an involutory (self-reciprocal) quagmire 4 cipher.

Introduction

The Porta cipher [1, 2] is a subset of an earlier Bellaso cipher of 1552. Each of its monoalphabetic keys is self-reciprocal (involutory), thus so is the full cipher. We will show that this cipher is isomorphic to the Beaufort, and is therefore also a quagmire 4 (Q4) cipher. We will provide some choices for the mixed alphabets on the plaintext and ciphertext sides of the Q4 (i.e., the "keywords"), and show that they are also the isomorphisms between Beaufort and Bellaso.

The Bellaso ciphers

The cipher known to us as the "Porta" is one of Giovan Battista Bellaso's polyalphabetic ciphers that was misattributed to another cryptographer. Bellaso's tableau [3] employs the 22-letter Italian alphabet of the time:

key letter	plaintext alphabet a b c d e f g h i l m n o p q r s t u x y z
A/B	N O P Q R S T U X Y Z A B C D E F G H I L M
C/D	T U X Y Z N O P Q R S F G H I L M A B C D E
E/F	Z N O P Q R S T U X Y B C D E F G H I L M A
G/H	S T U X Y Z N O P Q R G H I L M A B C D E F
I/L	Y Z N O P Q R S T U X C D E F G H I L M A B
M/N	R S T U X Y Z N O P Q H I L M A B C D E F G
O/P	X Y Z N O P Q R S T U D E F G H I L M A B C
Q/R	Q R S T U X Y Z N O P I L M A B C D E F G H
S/T	P Q R S T U X Y Z N O L M A B C D E F G H I
U/X	U X Y Z N O P Q R S T E F G H I L M A B C D
Y/Z	O P Q R S T U X Y Z N M A B C D E F G H I L

Recently, an earlier cipher of Bellaso from 1552 was uncovered in Venice, Italy [4]. Its tableau is a superset of the above:

key letter	plaintext alphabet a b c d e f g h i l m n o p q r s t u x y z
A	N O P Q R S T U X Y Z A B C D E F G H I L M
E	Z N O P Q R S T U X Y B C D E F G H I L M A
I	Y Z N O P Q R S T U X C D E F G H I L M A B
O	X Y Z N O P Q R S T U D E F G H I L M A B C
U	U X Y Z N O P Q R S T E F G H I L M A B C D
B	T U X Y Z N O P Q R S F G H I L M A B C D E
C	S T U X Y Z N O P Q R G H I L M A B C D E F
D	R S T U X Y Z N O P Q H I L M A B C D E F G
F	Q R S T U X Y Z N O P I L M A B C D E F G H
G	P Q R S T U X Y Z N O L M A B C D E F G H I
H	O P Q R S T U X Y Z N M A B C D E F G H I L
L	M L I H G F E D C B A Z Y X U T S R Q P O N
M	A M L I H G F E D C B Y X U T S R Q P O N Z
N	B A M L I H G F E D C X U T S R Q P O N Z Y
P	C B A M L I H G F E D U T S R Q P O N Z Y X
Q	D C B A M L I H G F E T S R Q P O N Z Y X U
R	E D C B A M L I H G F S R Q P O N Z Y X U T
S	F E D C B A M L I H G R Q P O N Z Y X U T S
T	G F E D C B A M L I H Q P O N Z Y X U T S R
X	H G F E D C B A M L I P O N Z Y X U T S R Q
Y	I H G F E D C B A M L O N Z Y X U T S R Q P
Z	L I H G F E D C B A M N Z Y X U T S R Q P O

The modern version, now called the “Porta cipher,” comes in two varieties, depending on where you live and what books you read. Their tableaux are combined here:

key letter v. 1	key letter v. 2	plaintext alphabet a b c d e f g h i j k l m n o p q r s t u v w x y z
A/B	A/B	N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
C/D	Y/Z	O P Q R S T U V W X Y Z N M A B C D E F G H I J K L
E/F	W/X	P Q R S T U V W X Y Z N O L M A B C D E F G H I J K
G/H	U/V	Q R S T U V W X Y Z N O P K L M A B C D E F G H I J
I/J	S/T	R S T U V W X Y Z N O P Q J K L M A B C D E F G H I
K/L	Q/R	S T U V W X Y Z N O P Q R I J K L M A B C D E F G H
M/N	O/P	T U V W X Y Z N O P Q R S H I J K L M A B C D E F G
O/P	M/N	U V W X Y Z N O P Q R S T G H I J K L M A B C D E F
Q/R	K/L	V W X Y Z N O P Q R S T U F G H I J K L M A B C D E
S/T	I/J	W X Y Z N O P Q R S T U V E F G H I J K L M A B C D
U/V	G/H	X Y Z N O P Q R S T U V W D E F G H I J K L M A B C
W/X	E/F	Y Z N O P Q R S T U V W X C D E F G H I J K L M A B
Y/Z	C/D	Z N O P Q R S T U V W X Y B C D E F G H I J K L M A

We suggest that the original Bellaso 1552 cipher can be modernized in a similar fashion. We expand the alphabet to include all 26 letters of the modern English alphabet, but do not assign key letters to the ciphertext alphabets because to do so would be arbitrary. We do, however, label them so that later we can refer to them easily. Notice again how each of the ciphertext alphabets is reciprocal. The full cipher is also reciprocal: encipherment and decipherment are the same process.

plaintext alphabet abcdefghijklmnopqrstuvwxyz
AMLKJIHGFEDCBYXWVUTSRQPONZ
BAMLKJIHGFEDCXWVUTSRQPONZY
CBAMLKJIHGFEDWVUTSRQPONZYX
DCBAMLKJIHGFEVUTSRQPONZYXW
EDCBAMLKJIHGFUTSRQPONZYXWV
FEDCBAMLKJIHGTSRQPONZYXWVU
GFEDCBAMLKJIHSRQPONZYXWVUT
HGFEDCBAMLKJIRQPONZYXWVUTS
IHGFEDCBAMLKJQPONZYXWVUTSR
JIHGFEDCBAMLKPONZYXWVUTSRQ
KJIHGFEDCBAMLONZYXWVUTSRQP
LKJIHGFEDCBAMNZYXWVUTSRQPO
MLKJIHGFEDCBAZYXWVUTSRQPON
NOPQRSTUVWXYZABCDEFGHIJKLM
OPQRSTUVWXYZNMABCDEFGHIJKL
PQRSTUVWXYZNOLMABCDEFGHIJK
QRSTUVWXYZNOPKLMABCDEFGHIJ
RSTUVWXYZNOPQJKLMABCDEFGHI
STUVWXYZNOPQRIJKLMABCDEFGH
TUVWXYZNOPQRSHIJKLMABCDEFG
UVWXYZNOPQRSTGHIJKLMABCDEF
VWXYZNOPQRSTUFGHIJKLMABCDE
WXYZNOPQRSTUVEFGHIJKLMABCD
XYZNOPQRSTUVWDEFGHIJKLMABC
YZNOPQRSTUVWXCDEFGHIJKLMAB
ZNOPQRSTUVWXYBCDEFGHIJKLMA

In previous work [5] we saw that there is a class of involutory (self-reciprocal) quagmire 4 (Q4) ciphers, and that each of these ciphers is simultaneously both a right and left coset of a single quagmire 3 (Q3). The Beaufort cipher (B) is a member of this class, and it is a coset of the Vigenère (V) itself.

The Beaufort cipher

The Beaufort cipher [1, 2] is another periodic polyalphabetic substitution cipher, and it is also self-reciprocal. Here is its tableau:

key letter	plaintext alphabet a b c d e f g h i j k l m n o p q r s t u v w x y z	label
A	AZYXWVUTSRQPONMLKJIHGFEDCB	b_{25}
B	BAZYXWVUTSRQPONMLKJIHGFEDC	b_{24}
C	CBAZYXWVUTSRQPONMLKJIHGFED	b_{23}
D	DCBAZYXWVUTSRQPONMLKJIHGFE	b_{22}
E	EDCBAZYXWVUTSRQPONMLKJIHGF	b_{21}
F	FEDCBAZYXWVUTSRQPONMLKJIHG	b_{20}
G	GFEDCBAZYXWVUTSRQPONMLKJIH	b_{19}
H	HGFEDCBAZYXWVUTSRQPONMLKJI	b_{18}
I	IHGFEDCBAZYXWVUTSRQPONMLKJ	b_{17}
J	JIHGFEDCBAZYXWVUTSRQPONMLK	b_{16}
K	KJIHGFEDCBAZYXWVUTSRQPONML	b_{15}
L	LKJIHGFEDCBAZYXWVUTSRQPONM	b_{14}
M	MLKJIHGFEDCBAZYXWVUTSRQPON	b_{13}
N	NMLKJIHGFEDCBAZYXWVUTSRQPO	b_{12}
O	ONMLKJIHGFEDCBAZYXWVUTSRQP	b_{11}
P	PONMLKJIHGFEDCBAZYXWVUTSRQ	b_{10}
Q	QPONMLKJIHGFEDCBAZYXWVUTSR	b_{9}
R	RQPONMLKJIHGFEDCBAZYXWVUTS	b_{8}
S	SRQPONMLKJIHGFEDCBAZYXWVUT	b_{7}
T	TSRQPONMLKJIHGFEDCBAZYXWVU	b_{6}
U	UTSRQPONMLKJIHGFEDCBAZYXWV	b_{5}
V	VUTSRQPONMLKJIHGFEDCBAZYXW	b_{4}
W	WVUTSRQPONMLKJIHGFEDCBAZYX	b_{3}
X	XWVUTSRQPONMLKJIHGFEDCBAZY	b_{2}
Y	YXWVUTSRQPONMLKJIHGFEDCBAZ	b_{1}
Z	ZYXWVUTSRQPONMLKJIHGFEDCBA	$b_{0} = z$

We have numbered them in backward order so that the subscript denotes the size of the leftward shift of the Atbash [6] key

$$z = \texttt{ZYXWVUTSRQPONMLKJIHGFEDCBA}$$

The individual monoalphabetic keys of the Vigenère cipher [1, 2, 7] are the rotations

$$\begin{aligned} R_0 &= \texttt{ABCDEFGHIJKLMNOPQRSTUVWXYZ} = e \\ R_1 &= \texttt{BCDEFGHIJKLMNOPQRSTUVWXYZA} \\ R_2 &= \texttt{CDEFGHIJKLMNOPQRSTUVWXYZAB} \\ &\vdots \\ R_{25} &= \texttt{ZABCDEFGHIJKLMNOPQRSTUVWXY} \end{aligned}$$

The Beaufort keys are compositions of these rotations with z; this is why we say that B is a coset of V. Composition of permutations is not commutative, but for R_n and z, changing the order merely reorders the rows of the resulting tableau; we consider that to be the same cipher.

$$b_n = z \circ R_n = R_{-n} \circ z$$

As promised, each of the keys is self-reciprocal:

$$b_n^2 = e$$

The Porta/Bellaso cipher is a quagmire 4

To show that the Porta/Bellaso cipher (P) is a member of the class of involutory quagmire 4s, we merely have to provide the alphabetic keys for the Q4 that reproduces the Bellaso tableau. Consider this permutation and its reversal:

x = AYCWEUGSIQKOMZBXDVFTHRJPLN
$x \circ z$ = NLPJRHTFVDXBZMOKQISGUEWCYA

The Q4 keys obtained with it for the set (see [8] for the factoring of a Q4 and why its keys are of the form $k_C \circ R_n \circ k_P^{-1}$)

$$\{x \circ z \circ R_n \circ x^{-1}\}$$

These are indeed the Bellaso keys. Furthermore,

$$P = \{x \circ (z \circ R_n) \circ x^{-1}\}$$

has the form of an isomorphism from B = $\{z \circ R_n\}$ to P. From this we rightly conclude that the Porta/Bellaso cipher is isomorphic to the Beaufort.

But why stop there? There is a number of such permutations that will serve this purpose. Recall the automorphisms of V [8]:

a_1 = ABCDEFGHIJKLMNOPQRSTUVWXYZ = e
a_3 = ADGJMPSVYBEHKNQTWZCFILORUX
a_5 = AFKPUZEJOTYDINSXCHMRWBGLQV
a_7 = AHOVCJQXELSZGNUBIPWDKRYFMT
a_9 = AJSBKTCLUDMVENWFOXGPYHQZIR
a_{11} = ALWHSDOZKVGRCNYJUFQBMXITEP
a_{15} = APETIXMBQFUJYNCRGVKZODSHWL
a_{17} = ARIZQHYPGXOFWNEVMDULCTKBSJ
a_{19} = ATMFYRKDWPIBUNGZSLEXQJCVOH
a_{21} = AVQLGBWRMHCXSNIDYTOJEZUPKF
a_{23} = AXUROLIFCZWTQNKHEBYVSPMJGD
a_{25} = AZYXWVUTSRQPONMLKJIHGFEDCB = b_{25}

They are the keys of shiftless affine ciphers. However, adding shifts (rotations) also transforms the Vigenère set into itself. Therefore, any permutation of the form

$$x \circ a_m \circ R_n$$

will work as our Q4 alphabetic key in order to produce the Porta/Bellaso tableau (the other key is its reversal). The only difference among them is that the tableau rows are listed in different order. And any of them will serve to define an isomorphism from B to P. After all,

$$\begin{aligned}(x \circ a_m \circ R_n) \circ z \circ R_k \circ (x \circ a_m \circ R_n)^{-1} &= x \circ a_m \circ R_n \circ z \circ R_k \circ R_{-n} \circ {a_m}^{-1} \circ x^{-1} \\ &= x \circ a_m \circ z \circ R_{-n} \circ R_k \circ R_{-n} \circ {a_m}^{-1} \circ x^{-1} \\ &= x \circ z \circ a_m \circ R_s \circ R_k \circ {a_m}^{-1} \circ x^{-1} \\ &= x \circ z \circ R_{m(k+s)} \circ x^{-1}\end{aligned}$$

where s depends in some way on m and the arithmetic in the subscripts is done modulo 26.

What then is the Q3 of which the P is a coset? It is the one having this set of keys:

plaintext alphabet

```
abcdefghijklmnopqrstuvwxyz
```

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ = e
BCDEFGHIJKLMAZNOPQRSTUVWXY
CDEFGHIJKLMABYZNOPQRSTUVWX
DEFGHIJKLMABCXYZNOPQRSTUVW
EFGHIJKLMABCDWXYZNOPQRSTUV
FGHIJKLMABCDEVWXYZNOPQRSTU
GHIJKLMABCDEFUVWXYZNOPQRST
HIJKLMABCDEFGTUVWXYZNOPQRS
IJKLMABCDEFGHSTUVWXYZNOPQR
JKLMABCDEFGHIRSTUVWXYZNOPQ
KLMABCDEFGHIJQRSTUVWXYZNOP
LMABCDEFGHIJKPQRSTUVWXYZNO
MABCDEFGHIJKLOPQRSTUVWXYZN
NZYXWVUTSRQPOLKJIHGFEDCBAM
ONZYXWVUTSRQPKJIHGFEDCBAML
PONZYXWVUTSRQJIHGFEDCBAMLK
QPONZYXWVUTSRIHGFEDCBAMLKJ
RQPONZYXWVUTSHGFEDCBAMLKJI
SRQPONZYXWVUTGFEDCBAMLKJIH
TSRQPONZYXWVUFEDCBAMLKJIHG
UTSRQPONZYXWVEDCBAMLKJIHGF
VUTSRQPONZYXWDCBAMLKJIHGFE
WVUTSRQPONZYXCBAMLKJIHGFED
XWVUTSRQPONZYBAMLKJIHGFEDC
YXWVUTSRQPONZAMLKJIHGFEDCB
ZYXWVUTSRQPONMLKJIHGFEDCBA = z
```

To generate this Q3, we use any of the alphabetic keys $x \circ a_m \circ R_n$ from above to create the set (again see [8] for an explanation of how Q3 keys are constructed)

$$\{x \circ R_n \circ x^{-1}\} \;=\; \{(x \circ a_m \circ R_n) \circ R_k \circ (x \circ a_m \circ R_n)^{-1}\}$$

We see that each of the 312 permutations of the form $x \circ a_m \circ R_n$ can be used as one of the Q4 keywords with its reversal as the other to obtain the Bellaso/Porta tableau, as the keyword for its partner Q3, and as an isomorphism between B and P.

Conclusion

The Porta cipher is a subset of the Bellaso 1552 cipher, which is an involutory quagmire 4. It is the right coset and left coset of the same quagmire 3. We explicitly presented one set of quagmire keywords that generate the Bellaso/Porta tableau, however, there are many choices for them. Furthermore, it is isomorphic to the Beaufort cipher.

References

[1] Helen Fouché Gaines, *Cryptanalysis: a study of ciphers and their solution*, New York: Dover, 1956; previously titled *Elementary Cryptanalysis* and published by American Photographic in 1939; http://archive.org/details/cryptanalysis00gain.

[2] American Cryptogram Association, The ACA and You, http://www.cryptogram.org/cdb/aca.info/aca.and.you/aca.and.you.pdf, 2005. The 2016 version is archived at http://web.archive.org/web/*/http://cryptogram.org/docs/acayou16.pdf. The relevant pages are also available as https://www.cryptogram.org/downloads/aca.info/ciphers/Beaufort.pdf, Porta.pdf, QuagmireI.pdf, QuagmireII.pdf, QuagmireIII.pdf, QuagmireIV.pdf, and Vigenere.pdf.

[3] Giovan Battista Bellaso, *La Cifra del Sig. Giouan Battista Belaso* [sic], 1553.

[4] Paolo Bonavoglia, Bellaso's 1552 cipher recovered in Venice, *Cryptologia* 43:6 (2019) 459-465, DOI: 10.1080/01611194.2019.1596181

[5] Thomas Kaeding, Quagmire ciphers and group theory: What is a Beaufort cipher?, Cryptology ePrint Archive, report 2022/1488.

[6] For lack of a better reference, https://en.wikipedia.org/wiki/Atbash.

[7] Blaise de Vigenère, *Traicté des chiffres ou secrètes manières d'escrire*, Paris: Abel l'Angelier, 1586, HDL: 2027/ien.35552000251008, http://gallica.bnf.fr/ark:/12148/bpt6k1040608n, http://gallica.bnf.fr/ark:/12148/bpt6k94009991.

[8] Thomas Kaeding, Quagmire ciphers, group theory, and information: Key amplification in crib-based attacks, Cryptology ePrint Archive, report 2022/1382.